REMARKS

The above-identified application is United States application serial number 10/676,541 filed on October 1, 2003. Claims 1-66 are pending in the application. Claims 1-66 are rejected. Applicant respectfully traverses these rejections to put the claims in form for appeal.

Rejection of Claims under 35 U.S.C. §101

Claims 1-66 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 as amended recites "a computer-implemented method comprising: observing communication between a plurality of devices; and inferring a respective state of at least one device of the plurality of devices based upon the observing the communication." The rejection states that the claim is clearly a software program and it is non-statutory as not being tangibly embodied in a manner so as to be executable and therefore recites a non-statutory subject matter. In response, Applicant refers to Section 2106.01 of the Manual of Patent Examining Procedure (MPEP), which provides:

> "When a computer program is claimed in a process where the computer is executing the computer program's instructions, USPTO personnel should treat the claim as a process claim."

Applicant therefore believes that claims 1-30 are statutory process claims. Removal of the rejection under 35 U.S.C. 101 is respectfully requested.

Applicant has amended claims 31-66 to recite tangible computer-readable medium. Removal of the rejection of claims 31-66 under 35 U.S.C. 101 is respectfully requested.

Rejection of Claims under 35 U.S.C. §102

Claims 1, and 3-12, 14-32, 34-44, 46-56, and 58-66 are rejected under 35 U.S.C. 102(e) as being anticipated by Carter *et al.* (US 200310051026). Claim 1 recites

> "observing communication between a plurality of devices; and
> inferring a respective state of at least one device of the plurality of devices based upon the observing the communication."

In contrast, one cited portion of Carter teaches an Event Learning subcomponent that observes the network's current state of security and incorporates information of a new outcome state that results from an initial known state of security encountering an event which has the potential to change that initial known state. (Carter paragraph [0219]). Claim 1 does not determine the state of the network, but rather a respective state for at least one of the devices. The devices may thus be assigned their own respective states, whereas Carter only determine one state for the network. Another cited portion of Carter teaches developing separate populations of problem solving processes by application of co-evolution, and determining the fitness of the constituents of the separate populations. (Carter paragraph [0242]). The determination of the constituents' fitness is based on their ability to accomplish specified results and on prior observations of network events. (Carter, *Id.*). Nothing in Carter discloses or suggests that a respective state is inferred for at least one device. Carter only determines the fitness of constituents that are part of a group of problem solving processes, not devices among which communication is being observed.

The Examiner further cited paragraph [0207] of Carter as teaching the respective state of a device. Applicant respectfully disagrees. The cited portion of Carter defines "stateful" as a computer or program that keeps track of the state of a sequence of interactions with a user, another computer or program, a device, or other outside element, usually by setting values in a storage field designated for that purpose. Keeping track of the interaction between elements in Carter is not the same

as inferring a state of at least one device based upon observing communication between a plurality of devices in claim 1.

Claim 1 is distinguishable from Carter for at least these reasons.

Claims 2-30 depend from claim 1 and include features that further distinguish them from the prior art. For example, claim 9 recites:

> "setting a designation for a first device of the at least one device to a possible threat based upon a packet configuration for a packet sent by the first device as part of the communication".

In contrast, paragraph [0787] of Carter teaches a list of observations made by the Network Surveillance and Security System. None of the observation events describe designating a device as a possible threat based upon the packet configuration sent by the device. Instead, Carter teaches determining the current security status of a system and predicting the future state of the system based on past security states. (Carter paragraphs [0260]-[0261]). Since Carter does not disclose or suggest setting or predicting a designation for a device based upon a packet configuration for a packet sent by the device, Claim 9 is distinguishable from the prior art for at least these additional reasons.

As a further example, claim 13 recites:

> "the respective state of the first device is determined to be unfulfilled
> when the observing the communication comprises
> observing an address resolution protocol request comprising a destination address for the first device, and
> observing that the first device does not respond to the address resolution protocol request prior to expiration of a time limit"

The cited portions of Carter do not disclose or suggest these features. Rather, Carter teaches TCP/IP functions of assembling messages into packets for transmission over a network. (Carter paragraph [0028]). (See Carter paragraph [0060] for a diagram of the OSI Reference Model with TCP/IP protocols in network layers 4 and 3, respectively).

Another cited portion of Carter describes a frame of data that is transmitted between network points complete with addressing and protocol control information. (Carter paragraph [0084]). Yet another cited portion of Carter describes operation of the Internet Protocol (IP). (Carter paragraph [0152]). Applicant has also reviewed Carter's teaching of identifying potential threats and resulting state transitions for a protected server constellation, as described by paragraphs [785]-[0866] and Figure 19, and paragraphs [1073]-[1090] and Figure 20 in Carter. Applicant finds no indication that Carter discloses or suggests changing the state of the first device when the first device does not respond to the address resolution protocol request prior to expiration of a time limit. Claim 13 is distinguishable from Carter for at least these reasons.

As another example, claim 23 recites:

> "wherein the respective state of the first device is determined to be omitted when the observing is programmed to omit communication with the first device from the observing."

Nothing in Carter teaches or suggests these features. One cited portion of Carter teaches that the NAI Learning component hypothesizes a theorem about the security state of the protected constellation, determines the validity of the theorem by comparing with observations, and incorporates into the knowledge base as facts those theorems which prove valid. (Carter paragraph [0461]). Another cited portion of Carter teaches use of Unix commands to obtain information relating to any user of the protected constellation. The information about the users is retrieved from the results of the constellation traffic audits. (Carter paragraph [0870]). Some of the default values of the commands are set to ignore the respective event, but the traffic audits are still performed for the device regardless of whether the events are ignored. (Carter paragraph [0966]). Carter thus does not teach or suggest the features of the state of the device being determined as omitted as set forth in claim 23.

Claims 31-42 were rejected with the same rationale applied against claims 1, 10-11, 13-14, 16-17, 19, 21, 23, and 26-27. Claims 31-42 are distinguishable from the

cited references for at least the same respective reasons provided for the claims 1, 13, and 23 above.

Claims 43-54 were rejected with the same rationale applied against claims 1, 10-11, 13-14, 16-17, 19, 21, 23, and 26-27. Claims 43-54 are distinguishable from the cited references for at least the same respective reasons provided for the claims 1, 13, and 23 above.

Claims 55-66 were rejected with the same rationale applied against claims 1, 10-11, 13-14, 16-17, 19, 21, 23, and 26-27. Claims 55-66 are distinguishable from the cited references for at least the same respective reasons provided for the claims 1, 13, and 23 above.

CONCLUSION

The application, including all remaining claims, is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephone interview, the examiner is requested to telephone the undersigned at (949) 350-7301.

I hereby certify that this correspondence is being electronically transmitted to the USPTO, on the date shown below:

/Mary Jo Bertani/
(Signature)

Mary Jo Bertani
(Printed Name of Person Signing Certificate)

October 12, 2007
(Date)

Respectfully submitted,

/Mary Jo Bertani/

Mary Jo Bertani
Attorney for Applicant(s)
Reg. No. 42321